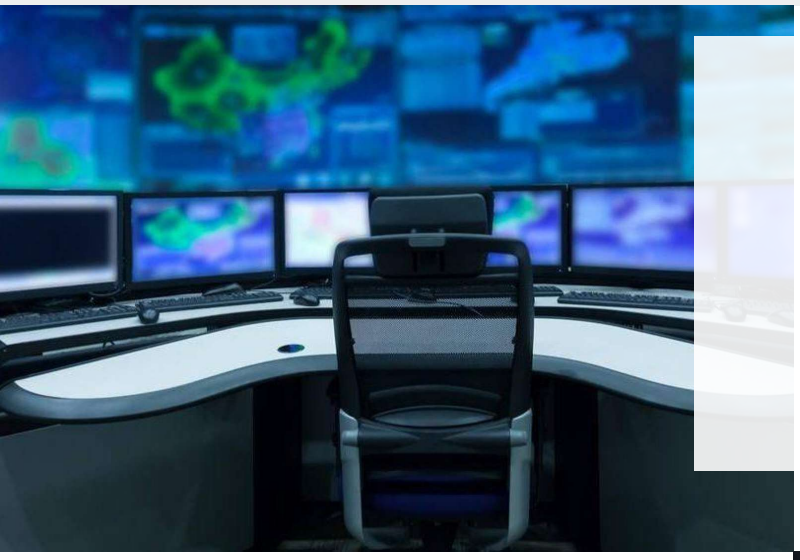
HELPING A LARGE SOLAR FARM BECOME SOCI COMPLIANT

"It takes less time to do a thing right than to explain why you did it wrong" - Henry Wadsworth Longfellow

Industry	Sector	Segment
Energy	Renewables	Solar



Project

The client, a large solar farm operator in Australia, faced a significant challenge with the recent amendments to the Security of Critical Infrastructure Act 2018 (SOCI Act). These changes mandated the development and maintenance of a Critical Infrastructure Risk Management Program (CIRMP) for assets in the energy sector. The solar farm, however, was not equipped with such a plan, risking non-compliance, potential penalties, and increased vulnerability to cyber threats.

The legal compliance with the SOCI Act was critical as non-compliance could lead to penalties. Additionally, the farm's cybersecurity risk was heightened due to the use of IoT devices and SCADA systems, necessitating robust risk management to ensure operational resilience.

Solution

To address these challenges, we engaged with the client through a series of workshops to educate and align stakeholders with the new regulatory demands and cybersecurity best practices. A gap analysis was conducted to assess the solar farm's cybersecurity posture against the CIRMP requirements, revealing deficiencies in risk identification and mitigation strategies.

We performed risk assessments using an "all hazards" approach, considering various threats that could affect the solar farm's operations. This led to the development of a full Critical Infrastructure Risk Management Plan. This plan included hazard identification, risk minimization strategies, specific mitigation plans, governance structures, and provisions for continuous improvement to adapt to new threats or regulatory changes.

Outcome

The outcomes of these efforts were significant. The solar farm achieved compliance with the SOCI Act's CIRMP requirements, thereby avoiding legal and financial repercussions. Security was enhanced, reducing cybersecurity vulnerabilities and improving operational security. Furthermore, demonstrating commitment to security governance reassured stakeholders, enhancing confidence from investors, customers, and regulatory bodies.

In conclusion, this case study demonstrates how compliance with the SOCI Act amendments not only addresses legal obligations but also strengthens the cybersecurity framework of critical infrastructure like solar farms. By adopting a comprehensive CIRMP, the solar farm not only met regulatory requirements but also set a precedent their other Assets in Australia.